AF
IFW

PATENT
Attorney Docket No. 53470.003026

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Number	: 09/883,509	Confirmation No.:	8697
Applicant	: Jeffrey Bedell *et al*		
Filed	: January 29, 2002		
Title	: Method and system for implementing security filters for reporting systems		
TC/Art Unit	: 2655		
Examiner:	: Christopher A. Revak		
Docket No.	: 53470.003026		
Customer No.	: **21967**		

SUBMISSION OF APPEAL BRIEF

Sir:

In response to the Office Action dated September 30, 2005 finally rejecting pending claims 1-18 and further in response to the Notice of Appeal filed on December 22, 2005, Appellant respectfully submits this Appeal Brief in connection with the above-captioned patent application in compliance with 37 C.F.R. § 1.192 (c).

Respectfully submitted,

HUNTON & WILLIAMS

By: _____
Ozzie A. Farres
Registration No. 43,606

Hunton & Williams
1900 K Street, N.W., Suite 1200
Washington, D.C. 20006-1109
(202) 955-1500

Dated: March 22, 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	)	
Jeffrey A. BEDELL, et al.	)	Group Art Unit: 2131
	)	
Serial Number: 09/883,509	)	Examiner: Christopher A. Revak
	)	
Filed: June 19, 2001	)	
	)	
Attorney Docket No. 53470.003026	)	
	)	
	)	
For: METHOD AND SYSTEM FOR IMPLEMENTING SECURITY FILTERS FOR REPORTING SYSTEMS	)	

APPEAL BRIEF

TABLE OF CONTENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	)	
Jeffrey A. BEDELL, et al.	)	Group Art Unit: 2131
	)	
Serial Number: 09/883,509	)	Examiner: Christopher A. Revak
	)	
Filed: June 19, 2001	)	
	)	
Attorney Docket No. 53470.003026	)	
	)	
	)	
For: SYSTEM AND METHOD FOR IMPLEMENTING SECURITY FILTERS FOR REPORTING SYSTEMS	)	

APPEAL BRIEF

In response to the Office Action dated September 30, 2005, finally rejecting pending claims 1-18, appellants respectfully request that the Board of Patent Appeals and Interferences reconsider and withdraw the rejections of record, and allow the pending claims, which are attached hereto as an Appendix A.

I. REAL PARTY IN INTEREST

The real party in interest is Microstrategy, Inc., the assignee of the above-referenced application.

II. RELATED APPEALS AND INTERFERENCES

There are no known related appeals or interferences.

III. STATUS OF CLAIMS

Claims 1-18 are pending in this application. The rejection of claims 1-18 is appealed.

IV. STATUS OF AMENDMENTS

No amendments to the claims have been filed subsequent to the final rejection dated

V. SUMMARY OF INVENTION

Appellants believe that a brief discussion of the background technology, followed by a brief summary of the embodiments of the invention and the problems solved by the embodiments of the present invention, will assist the Board of Patent Appeals and Interferences (hereinafter referred to as "the Board") in appreciating the significant advances made by the embodiments of the present invention. Finally, concise explanations of each of the independent claims are provided, including reference to exemplary portions of the specification and figures.

A. The Background

Decision support systems have been developed to efficiently retrieve selected information from data warehouses. One type of decision support system is known as an on-line analytical processing system (OLAP). Other systems may include Business Intelligence and reporting systems. In general, OLAP systems analyze the data from a number of different perspectives and support complex analyses against large input data sets. OLAP systems generally output upon execution of a report that inputs a template to indicate the way to present the output and a filter to specify the conditions of data on which the report is to be presented.

Security is a major concern in any system. Large systems typically provide users with access to a wealth of information, not all of which is meant to be seen by everyone. In general, security systems may have the components related to authentication, access control and auditing. Authentication may include a method for identifying a user to the system. Access control may involve what the user is allowed to see and do once the user has been identified. Auditing may include a record of the data the user viewed and actions the user performed. Security may be generally implemented in various areas of a system, which may include databases,

network/operating systems, and various applications.

Security at the database level is extremely important because anyone can bypass traditional security measures by using a simple, non-secure query tool to access the database or databases. The network generally controls access to a computer while the operating system controls access to the files and applications that are stored in a particular computer. It is important to protect computers, sensitive files and other information from inadvertent or malicious tampering.

B. The Embodiments of The Present Invention

Security at the data level may regulate access to data associated with underlying systems and/or applications. Access to data may be monitored by security filters and other mechanisms. Security filters may apply when a user attempts to access information via a query or other user input. For example, the user may receive information filtered on what the user is allowed to view even if the user asks for a greater scope of information. *See Page 2, lines 12-16.*

Security filters may be implemented to prevent users from viewing or otherwise accessing certain data in a database or other source of information. For example, if two users with different security filters run the exact same report, each user may receive different results because each user may have different levels of security or access. The type of security filter may be based on a user's role, capabilities, or other criteria. For example, a regional manager may have a security filter that allows a user to view data from the user's particular region regardless of the report the user runs. The type of data the user may be allowed to view (or access) may be determined by various factors associated with a user's level of security, for example. *See Page 2, lines 17-22 - Page 3, lines 1-2.*

The present invention provides system and method for implementing a security filter for

regulating access to data associated with a reporting system, wherein a user submits a user identification input and a user request to the reporting system. The system may identify the user based on user identification input and retrieve data in accordance with the user request. The system may filter the retrieved data based on at least one security filter associated with the identified user and present the data to the user through a user interface. In another embodiment of the present invention, the user may be associated with a group of users wherein the security filter may include a group level security filter. The security filter may further incorporate data related to at least one of roles and privileges associated with the user. In addition, the security filter may incorporate access right data associated with the user. *See Page 3 lines 3-12.*

A security filter may include one or more of a filter expression, a top level and a bottom level. Other elements may be included. A filter expression may specify a subset of data that a user may be authorized to analyze. A top level may specify the highest level of analysis to which the security filter may be applied. If a top level is not defined, the security filter may apply to any level that is higher than the bottom level. A bottom level may specify the lowest level of analysis to which this security filter may be applied. If a bottom level is not defined, the security filter may apply to any level that is lower than the top level. When neither top level nor bottom level is specified, the security filter may be applied to each level of analysis. *See Page 3, lines 13-20.*

A user may submit a request for a report or other output. The system may then identify the user submitting the request and any intended recipients, if applicable. In addition, security levels and other security attributes may be associated with the identified entities (e.g., users, recipients, etc.). The report (or request) may be processed wherein the results may be subjected to one or more security filters to filter the results before presenting to the user or one or more

intended recipients. *See Page 3, lines 21-22 - Page 4, lines 1-4.*

C. Explanation of Independent Claim 1

A method for implementing a security filter (Figure 7; Page 20, lines 13-22 - Page 21, lines 1-3) for regulating access to data associated with a reporting system, comprising the steps of:

enabling a user to submit a user identification input (710, 1210; Page 20, lines 14-15) and a user request (204, 714; Page 20, lines 17-21) to an on-line analytical processing system (100; Page 6, lines 3-14);

identifying the user based on user identification input (712, 1118, 1214; Page 20, lines 14-17);

retrieving data associated with the on-line analytical processing system in accordance with the user request (220, 716; Page 20, lines 21-22);

filtering the retrieved data based on at least one security filter associated with the identified user (212, Fig. 6, 716; Page 20, lines 22 - Page 21, line 1); and

presenting the data as a report to the user through a user interface (226, 310, 718; Page 21, lines 1-2).

D. Explanation of Independent Claim 7

A system for implementing a security filter (332, Figure 4, Figure 5; Page 20, lines 13-22 - Page 21, lines 1-3) for regulating access to data associated with a reporting system (100; Page 5, line 21-22), comprising:

a user input (310) for enabling a user to submit a user identification input (1210; Page 20, lines 14-15) and a user request (312; Page 20, lines 17-18) to an on-line analytical processing system (100; Page 6, lines 3-14);

an identification module for identifying the user based on user identification input (344;

Page 20, lines 15-17);

an access module for retrieving data associated with the on-line analytical processing system in accordance with the user request (103; Page 20, lines 18-22);

at least one security filter for filtering the retrieved data wherein the at least one security filter is associated with the identified user (Figure 6; Page 20, line 22 - Page 21, lines 1-3); and

a user interface for presenting the data as a report to the user (110; Page 11, lines 1-4).

E. Explanation of Independent Claim 13

A processor-readable medium comprising code for execution by a processor to implement a security filter for regulating access to data associated with a reporting system (332, Figure 4, Figure 5; Page 12, lines 19-22 - Page 13, lines 1-12), the medium comprising:

code for causing a processor to enable a user to submit a user identification input (344; Page 20, lines 15-17) and a user request to an on-line analytical processing system (312, 714; Page 20, lines 17-21);

code for causing a processor to identify the user based on user identification input (712, 1118; Page 20, lines 15-17);

code for causing a processor to retrieve data associated with the on-line analytical processing system in accordance with the user request (220, 716; Page 20, lines 21-22);

code for causing a processor to filter the retrieved data based on at least one security filter associated with the identified user (Figure 6; Page 20, line 22 - Page 21, lines 1-3); and

code for causing a processor to present the data as a report to the user through a user interface (110; Page 11, lines 1-4).

VI. Grounds of Rejection to be Reviewed on Appeal

The issues on appeal are whether the following rejections are proper: (1) the rejection

under 35 U.S.C. § 112 of claims 1-18, (2) the rejection under 35 U.S.C. § 102(b) of Claims 1, 7 and 13 as being anticipated by Willens, U.S. Patent 5,889,958 ("Willens"), (3) the rejection under 35 U.S.C. § 103(a) of Claims 2-4, 6, 8-10, 12, 14-16 and 18 as being unpatentable under Willens in view of Pennock et al, U.S. Patent 6,484,168 ("Pennock") and (4) the rejection under 35 U.S.C. § 103(a) of Claims 5, 11 and 17 over Willens in view of Reid et al, U.S. Patent 6,182226 ("Reid").

VII. ARGUMENT

A. The Rejection Under 35 U.S.C. §112 of Claims 1-18 is improper

On Page 3 of the Office Action Claims 1-18 were rejected under 35 U.S.C. § 112, second paragraph as being indefinite for failing to point out and distinctly claim the subject matter which the applicant regards as the invention. Appellants respectfully traverse this rejection and submit that an on-line analytical processing system specified in the body of Claims 1, 7 and 13 is more limiting language describing a particular embodiment of a reporting system as specified in the corresponding preambles of Claims 1, 7 and 13. The specification discloses an on-line analytical processing system as an example of one type of reporting system. ("Fig 1. and Fig 2 provide an example of a reporting system, such as an OLAP system, in accordance with the present invention." Page 5, lines 21-22; Page 1, lines 5-6, "reporting systems, such as decision support, Business Intelligence, on-line analytical processing and other systems".) See Also MPEP § 2173.01. " A fundamental principal contained under 35 U.S.C. 112, second paragraph is that applicants are their own lexicographers. They can define in the claims what they regard as their own invention in whatever terms they choose so long as any special meaning in a term is clearly set forth in the specification."

In view of the above, appellants submit that the terms "reporting system" used in the

preamble of Claims 1, 7 and 13 and "on-line analytical processing system" as used in the bodies of Claims 1, 7 and 13 do not result in indefiniteness for failing to point out and distinctly claim the subject matter which the applicant regards as his invention. Accordingly, Appellants respectfully submit that the indefiniteness rejections of claims 1-18 are improper and respectfully request that they be withdrawn.

B. The Rejection Under 35 U.S.C. § 102(b) of Claims 1, 7 and 13 Based on U.S. Patent 5,889,958 ("Willens") is Improper

On Page 3 of the Office Action Claims 1, 7 and 13 were rejected under 35 U.S.C. § 102(b) as being anticipated by Willens. The Office Action alleges that each and every claimed limitation is shown by Willens. Applicants respectfully disagree.

Under 35 U.S.C. § 102, the Patent Office bears the burden of presenting at least a prima facie case of anticipation. In re Sun, 31 USPQ2d 1451, 1453 (Fed. Cir. 1993) (unpublished). Anticipation requires that a prior art reference disclose, either expressly or under the principles of inherency, each and every element of the claimed invention. Id.. "In addition, the prior art reference must be enabling." Akzo N.V. v. U.S. International Trade Commission, 808 F.2d 1471, 1479, 1 USPQ2d 1241, 1245 (Fed. Cir. 1986), cert. denied, 482 U.S. 909 (1987). That is, the prior art reference must sufficiently describe the claimed invention so as to have placed the public in possession of it. In re Donohue, 766 F.2d 531, 533, 226 USPQ 619, 621 (Fed. Cir. 1985). "Such possession is effected if one of ordinary skill in the art could have combined the publication's description of the invention with his own knowledge to make the claimed invention." Id..

Regarding independent claims 1, 7 and 13, the Examiner asserts that the network access server disclosed by Willens comprises the claimed on-line analytical processing system. The

network access server disclosed by Willens (col. 1, lines 6-13; col 2, lines 50-61; col. 3, lines 16-20 & col. 9, lines 17-21) refers to user access filters as part of an access control system for controlling access to the Internet. Any analysis done by the Willens access server is limited to whether access to a particular Internet site is allowed or denied. The claimed invention recites "retrieving data associated with the on-line analytical processing system." For instance, the specification of the claimed invention discloses on-line analytical processing systems as a systems which "analyze data from a number of different perspectives and support complex analyses against large input data sets." (Page 1, lines 14-15) Further an embodiment of the current invention discloses an on-line analytical processing system by which "users may query or interrogate a plurality of databases or database arrays to identify strategic trends." (Page 6, lines 8-10).

In view of the above, Appellants respectfully submit that Willens does not teach or suggest an on-line analytical processing system, it therefore does not teach or suggest the "retrieving data associated with an on-line analytical processing system" recited in Claims 1 and 7 or the "code for causing a processor to retrieve data associated with an on-line analytical processing system" recited in Claim 13 and thus cannot be relied on to reject Claims 1, 7 and 13 under 35 U.S.C. § 102(b).

The Examiner alleges filtering disclosed by Willens comprises "filter[ing] the retrieved data" as recited in claims 1, 7 and 13. The filtering disclosed by Willens is filtering of Internet sites(col. 2, lines 50-61) and is limited to the filtering of Internet sites. There is no on-line analytical processing system disclosed by Willens. The specification of the claimed invention discloses on-line analytical processing systems as a systems which "analyze data from a number of different perspectives and support complex analyses against large input data sets." (Page 1,

lines 14-15)

In view of the above, Appellants respectfully submit that Willens does not teach or suggest the "filter[ing] the retrieved data" as recited in claims 1, 7 and 13 and thus cannot be relied on to reject Claims 1, 7 and 13 under 35 U.S.C. § 102(b).

The Examiner further alleges the access notification system disclosed by Willens comprises the "presenting the data as a report to the user through the user interface" as recited in claim 1 or the similar limitations recited in claims 7 and 13 of the present application. The access notification system disclosed by Willens presents a notification as to whether access is allowed or denied. (col. 4, lines 58-62 & col. 5, lines 9-21). The notification system disclosed by Willens does not format or control the presentation of data that is returned for a user request. It is limited to a notification to the user as to whether the user request is allowed or denied. The specification of the claimed inventions discloses "a report that inputs a template to indicate the way to present the output" (page 1, line 16). The output referred to is the data returned by the query submitted by the user not the results of any security filtering. (Figure 2, 222, 224, 226).

In view of the above, Appellants respectfully submit that Willens does not teach or suggest the "presenting the data as a report to the user through the user interface" recited in Claim 1 or the similar limitations recited in claims 7 and 13 and thus cannot be relied on to reject Claims 1, 7 and 13 under 35 U.S.C. § 102(b).

For the above reasons Appellants respectfully request that the anticipation rejection of Claims 1, 7 and 13 be withdrawn .

C. The Rejection Under 35 U.S.C. § 103(a) of Claims 2-4, 6, 8-10, 12, 14-16 as being unpatentable under Willens in view of Pennock et al, U.S. Patent 6,484,168 ("Pennock") is Improper

Claims 2-4, 6, 8-10, 12, 14-16 and 18 are presently rejected under 35 U.S.C. § 103(a) as

allegedly being unpatentable over Willens in view of U.S. Patent No. 6,484,168 to Pennock *et al* ("Pennock"). Appellants respectfully disagree.

When a primary reference is missing elements, the law of obviousness requires that the Office set forth some motivation why one of ordinary skill in the art would have been motivated to modify the primary reference in the exact manner proposed. *Ruiz v. A.B. Chance Co.*, 234 F.3d 654, 664 (Fed. Cir. 2000). In other words, there must be some recognition that the primary reference has a problem and that the proposed modification will solve that exact problem. All of this motivation must come from the teachings of the prior art to avoid impermissible hindsight looking back at the time of the invention.

The mere fact a reference can be modified does not render the resultant modification obvious unless there is a suggestion or motivation found somewhere in the prior art regarding the desirability of the combination or modification. *See* M.P.E.P § 2143.01*; see also In re Mills*, 16 U.S.P.Q.2d 1430, 1432 (Fed. Cir. 1990); *In re Fritz*, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). In addition, the teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in Applicants' disclosure. *In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991).

The Office Action acknowledges that Willens does not disclose all the limitations as recited in the claims. For example, regarding Claims 2-4, 6, 8-10 and 14-16 the Office Action acknowledges that "The teachings of Willens fails to disclose that the security filter comprises a filter expression that specifies a subset of data in the database and has a top range and bottom range attribute that specifies the highest and lowest levels of analysis for applying the security filter." (Office Action, Page 4). As discussed in detail above Willens fails to show the combination of claim limitations as recited in independent claims 1, 7 and 13. For example,

Willens fails to disclose at least the limitations directed to an on-line analytical processing system, filtering the data retrieved from an on-line analytical processing system and presenting data as a report through an interface.

The Office Action alleges that Pennock discloses each of the above recitations. Appellants respectfully submit that Pennock fails to make up for Willens' deficiencies in this regard. Below are specific reasons why each of Claims 2-4, 6, 8-10, 12, 14-16 and 18 are separately patentable over Willens and Pennock.

1. Claims 2, 8 and 14 are Separately Patentable

Claims 2, 8 and 14 are separately patentable because there is no teaching or suggestion that either Willens or Pennock provide "a filter expression that specifies a subset of data in at least one database". The cited portion in Pennock refers to "a sequence of word filters" capable of filtering words out of documents so that only the relevant words characterizing the document remain in a word set (col. 2, lines 59-63). Pennock does not mention "a filter expression". Data in the present claims is not limited to words and expressions in the present claims do not equate to word lists. For these additional reasons Claims 2, 8 and 14 are separately patentable.

2. Claims 3, 9 and 15 are Separately Patentable

Claims 3, 9 and 15 are separately patentable because there is no teaching or suggestion that either reference provides a security filter with a "top range attribute that specifies the highest level of analysis to which the security filter is applied". The cited portion in Pennock refers to a frequency filter which counts the number of occurrences of a word within a database and eliminates words with occurrences above and below a certain range (col.3 , lines 22-25). The frequency filter disclosed in Pennock is limited to eliminating words from a word list that occur above and below a certain range. Pennock does not mention being able to use a top range

attribute to limit the highest level analysis. For this additional reason Claims 3, 9 and 15 are separately patentable.

3. Claims 4, 10 and 16 are Separately Patentable

Claims 4, 10 and 16 are separately patentable because there is no teaching or suggestion that either reference provides a security filter with a "bottom range attribute that specifies the lowest level of analysis to which the security filter is applied". The cited portion in Pennock refers to a frequency filter which counts the number of occurrences of a word within a database and eliminates words with occurrences above and below a certain range (col.3 , lines 22-25). The frequency filter disclosed in Pennock is limited to eliminating words from a word list that occur above and below a certain range. Pennock does not mention being able to use a bottom range attribute to limit the lowest level of analysis. For this additional reason Claims 4, 10 and 16 are separately patentable.

4. Claims 6, 12 and 18 are Separately Patentable

Claims 6, 12 and 18 are separately patentable because there is no teaching or suggestion that either Willens or Pennock provide "filter that varies by user and at least one fact/metric element". Willens' filters are based on network access rules and not a "fact/metric element". For this additional reason Claims 6, 12 and 18 are separately patentable.

5. No Motivation to Combine

Further, Appellants respectfully submit that the Office Action has failed to provide proper motivation for combining the Willens and Pennock references. Willens does not contemplate filtering data retrieved from an on-line analytical processing system using a "filter expression", a "top range attribute that specifies the highest level of analysis to which the security filter is applied" or a "bottom range attribute that specifies the lowest level of analysis to

which the security filter is applied". Pennock contemplates filtering documents based on a word list to reduce the size of individual documents to create a relevancy matrix. Pennock does not contemplate filtering data. Thus, there is no suggestion taught for a person of ordinary skill in the art to combine the Internet access mechanism disclosed in Willens with the document indexing mechanism disclosed in Pennock to achieve the claimed invention. Willens does not teach the use of a "filter that varies by user and at least one fact/metric element". Willens' filters are based on network access rules and not a "fact/metric element". For the above reasons Appellants respectfully request that the obviousness rejection of Claims 2-4, 6, 8-10, 12, 14-16 and 18 be withdrawn

D. The Rejection Under 35 U.S.C. § 103(a) of Claims 5, 11 and 17 as being unpatentable under Willens in view of U.S. Patent No. 6,182,226 to Reid *et al* ("Reid") is Improper

Claims 5, 11 and 17 are presently rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Willens in view of U.S. Patent No. 6,182,226 to Reid *et al* ("Reid"). Appellants respectfully disagree.

When a primary reference is missing elements, the law of obviousness requires that the Office set forth some motivation why one of ordinary skill in the art would have been motivated to modify the primary reference in the exact manner proposed. *Ruiz v. A.B. Chance Co.*, 234 F.3d 654, 664 (Fed. Cir. 2000). In other words, there must be some recognition that the primary reference has a problem and that the proposed modification will solve that exact problem. All of this motivation must come from the teachings of the prior art to avoid impermissible hindsight looking back at the time of the invention.

The mere fact a reference can be modified does not render the resultant modification obvious unless there is a suggestion or motivation found somewhere in the prior art regarding the

desirability of the combination or modification. *See* M.P.E.P § 2143.01; *see also In re Mills*, 16 U.S.P.Q.2d 1430, 1432 (Fed. Cir. 1990); *In re Fritz*, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). In addition, the teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in Applicants' disclosure. *In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991).

The Office Action acknowledges that Willens does not disclose all the limitations as recited in the claims. For example, regarding Claims 5, 11 and 17 the Office Action acknowledges "[t]he teachings of Willens are silent in disclosing that the user is associated with a group of users and applying a group level security filter"(Office Action, Page 5). As discussed in detail above Willens fails to show the combination of claim limitations as recited in independent claims 1, 7 and 13. For example, Willens fails to disclose at least the limitations directed to an on-line analytical processing system, filtering the data retrieved from an on-line analytical processing system and presenting data as a report through an interface.

The Office Action alleges that Reid discloses "wherein the user is associated with a group of users wherein the security filter is a group level security filter". Appellants respectfully submit that Reid fails to make up for Willens' deficiency in this regard. Below are specific reasons why each of Claims 5, 11 and 17 are separately patentable over Willens and Reid.

1. Claims 5, 11 and 17 are Separately Patentable

Claims 5, 11 and 17 are separately patentable because there is no teaching or suggestion that either Willens or Reid provide a security filter that is a group level security filter capable of filtering data. The group security filter disclosed in Reid is a network access filter not a data filter. For this additional reason Claims 5, 11 and 17 are separately patentable.

2. No Motivation to Combine

Further, Appellants respectfully submit that the Office Action has failed to provide proper motivation for combining the Willens and Reid references. Willens does not contemplate filtering data retrieved from an on-line analytical processing system using a filter "wherein the user is associated with a group of users wherein the security filter is a group level security filter. Willens contemplates a network access filter. Reid contemplates a group level network access filter. There is no motivation to combine a Willens and Reid to provide a group level security filter for filtering data. For the above reasons Appellants respectfully request that the obviousness rejection of Claims 5, 11 and 17 be withdrawn

CONCLUSION

It is respectfully submitted that this application and all pending claims are in condition for allowance and such disposition is earnestly solicited. If the Examiner believes that prosecution and allowance of the application will be expedited through an interview, whether personal or telephonic, the Examiner is invited to telephone the undersigned with any suggestions leading to the favorable disposition of the application.

The Director is hereby authorized to treat any current or future reply, requiring a petition for an extension of time for its timely submission as incorporating a petition for extension of time for the appropriate length of time. Applicants also authorize the Director to credit and differences or overpayment of fees to the undersigned's Deposit Account No. 50-0206.

Respectfully submitted,

March 22, 2006

Brian M. Buroker
Registration No. 39,125

Hunton & Williams, LLP
1900 K. St., NW, Suite 1200
Washington, D.C. 20006-1109
Tel. (202) 955-1894
Fax (202) 778-2201

VIII. CLAIMS APPENDIX

1. (Previously Presented) A method for implementing a security filter for regulating access to data associated with a reporting system, comprising the steps of:

enabling a user to submit a user identification input and a user request to an on-line analytical processing system;

identifying the user based on user identification input;

retrieving data associated with the on-line analytical processing system in accordance with the user request;

filtering the retrieved data based on at least one security filter associated with the identified user; and

presenting the data as a report to the user through a user interface.

2. (Original) The method of claim 1 wherein the security filter comprises a filter expression that specifies a subset of data in at least one database.

3. (Original) The method of claim 2 wherein the security filter comprises a top range attribute that specifies a highest level of analysis to which the security filter is applied.

4. (Original) The method of claim 2 wherein the security filter comprises a bottom range attribute that specifies a lowest level of analysis to which the security filter is applied.

5. (Original) The method of claim 1 wherein the user is associated with a group of users wherein the security filter is a group level security filter.

6. (Original) The method of claim 2 wherein the security filter varies by user and at least one fact/metric element.

7. (Previously Presented) A system for implementing a security filter for regulating access to data associated with a reporting system, comprising:

a user input for enabling a user to submit a user identification input and a user request to an on-line analytical processing system;

an identification module for identifying the user based on user identification input;

an access module for retrieving data associated with the on-line analytical processing system in accordance with the user request;

at least one security filter for filtering the retrieved data wherein the at least one security filter is associated with the identified user; and

a user interface for presenting the data as a report to the user.

8. (Original) The system of claim 7 wherein the security filter comprises a filter expression that specifies a subset of data in at least one database.

9. (Original) The system of claim 8 wherein the security filter comprises a top range attribute that specifies a highest level of analysis to which the security filter is applied.

10. (Original) The system of claim 8 wherein the security filter comprises a bottom range attribute that specifies a lowest level of analysis to which the security filter is applied.

11. (Original) The system of claim 7 wherein the user is associated with a group of users wherein the security filter is a group level security filter.

12. (Original) The system of claim 8 wherein the security filter varies by user and at least one fact/metric element.

13. (Previously Presented) A processor-readable medium comprising code for execution by a processor to implement a security filter for regulating access to data associated with a reporting system, the medium comprising:

code for causing a processor to enable a user to submit a user identification input and a user request to an on-line analytical processing system;

code for causing a processor to identify the user based on user identification input;

code for causing a processor to retrieve data associated with the on-line analytical processing system in accordance with the user request;

code for causing a processor to filter the retrieved data based on at least one security filter associated with the identified user; and

code for causing a processor to present the data as a report to the user through a user interface.

14. (Original) The medium of claim 13 wherein the security filter comprises a filter expression that specifies a subset of data in at least one database.

15. (Original) The medium of claim 14 wherein the security filter comprises a top range attribute that specifies a highest level of analysis to which the security filter is applied.

16. (Original) The medium of claim 14 wherein the security filter comprises a bottom range attribute that specifies a lowest level of analysis to which the security filter is applied.

17. (Original) The medium of claim 13 wherein the user is associated with a group of users wherein the security filter is a group level security filter.

18. (Original) The medium of claim 14 wherein the security filter varies by user and at least one fact/metric element.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.